

# Gebruik OpenAPI om informatie over ISE-certificaten op te halen op ISE 3.3

## Inhoud

---

[Inleiding](#)

[Achtergrond](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie op ISE](#)

[Python-voorbeelden](#)

[Ontvang alle systeemcertificaten van een bepaald knooppunt](#)

[Systeemcertificaat van een bepaald knooppunt verkrijgen via ID](#)

[Een lijst met alle vertrouwde certificaten opvragen](#)

[Vertrouwenscertificaat per ID verkrijgen](#)

[Problemen oplossen](#)

---

## Inleiding

Dit document beschrijft de procedure voor het gebruik van openAPI om het Cisco Identity Services Engine (ISE)-certificaat te beheren.

## Achtergrond

Geconfronteerd met toenemende complexiteit op het gebied van netwerkbeveiliging en -beheer voor ondernemingen, introduceert Cisco ISE 3.1 OpenAPI-geformatteerde API's die het beheer van de levenscyclus van certificaten stroomlijnen, en een gestandaardiseerde en geautomatiseerde interface bieden voor efficiënte en veilige certificaatbewerkingen, waardoor beheerders sterke beveiligingsprocedures kunnen afdwingen en netwerknaleving kunnen handhaven.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Services Engine (ISE)
- REST API

- Python

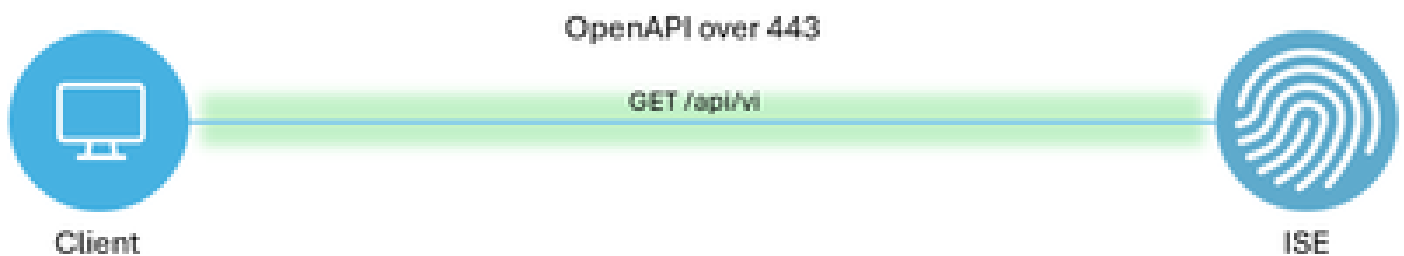
## Gebruikte componenten

- ISE-lijnkaart 3.3
- Python 3.10.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Configureren

### Netwerkdigram

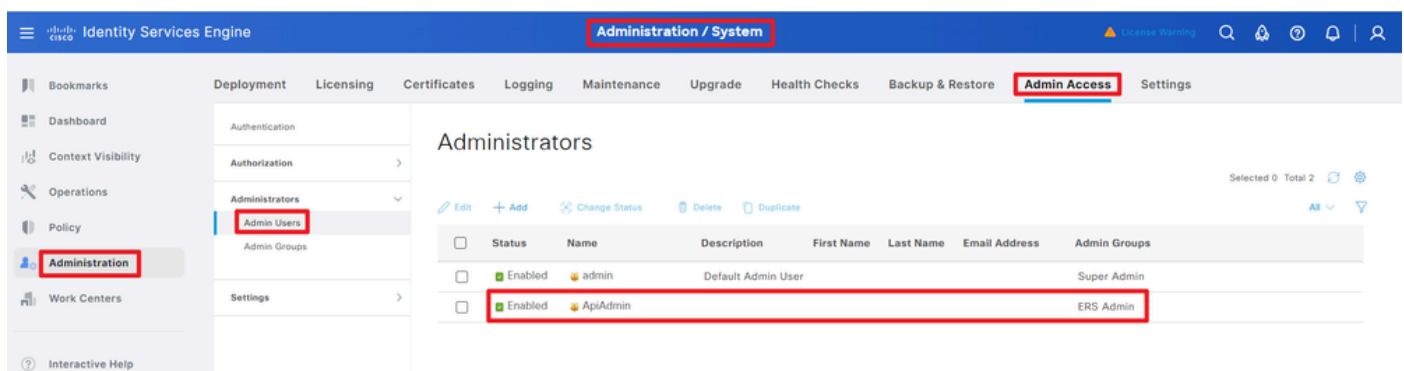


Topologie

### Configuratie op ISE

Stap 1: Voeg een Open API Admin account toe

Om een API-beheerder toe te voegen, navigeer naar Beheer > Systeem > Admin Access > Beheerders > Admin Gebruikers > Add.

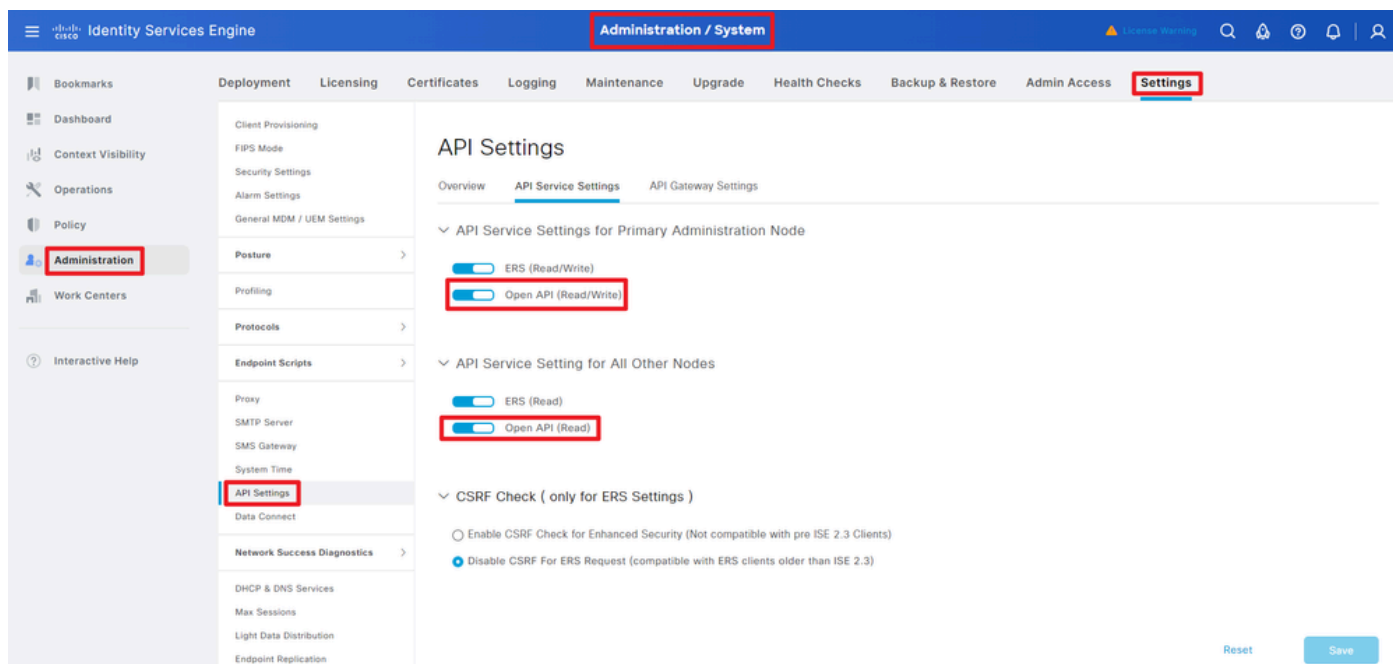


API-beheerder

Stap 2: Open API inschakelen op ISE

Open API is standaard uitgeschakeld op ISE. Om het in te schakelen, navigeer naar Beheer > Systeem > Instellingen > API-instellingen > API-serviceinstellingen. Schakel de opties voor Open

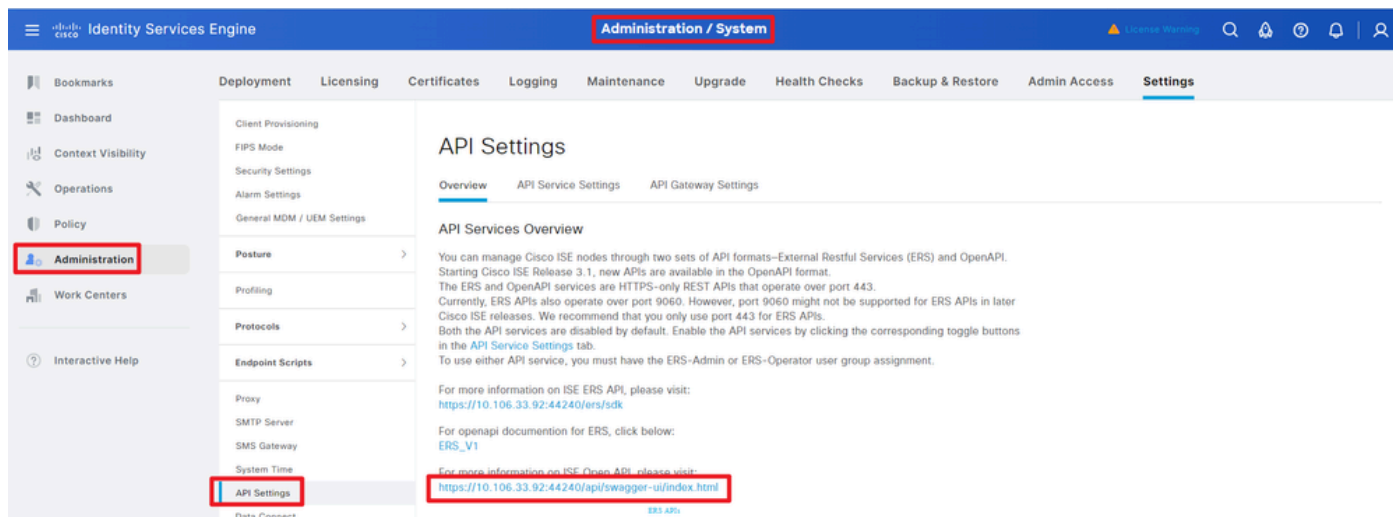
API in. Klik op Save (Opslaan).



OpenAPI inschakelen

Stap 3: Verken de open API van ISE

Ga naar Beheer > Systeem > Instellingen > API-instellingen > Overzicht. Klik op Open API bezoek link.



Bezoek OpenAPI

## Python-voorbeelden

Ontvang alle systeemcertificaten van een bepaald knooppunt

De API geeft een lijst van alle certificaten van een bepaald ISE-knooppunt.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
---------	---------

URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om certificaten van een bepaalde ISE-knooppunt op te halen.

The screenshot shows the Swagger UI for the Cisco ISE API - Certificates. The 'Certificates' section is highlighted with a red box. The endpoint '/api/v1/certs/system-certificate/{hostname}' is also highlighted with a red box. The interface includes a 'Servers' dropdown, a 'Select a definition' dropdown, and a list of API endpoints with their methods and descriptions.

API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

```
<#root>
```

```
from requests.auth import HTTPBasicAuth
import requests
```

```
requests.packages.urllib3.disable_warnings()
```

```
if __name__ == "__main__":
```

```
    url = "
```

```
https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN
```

```

"
  headers = {
"Accept": "application/json", "Content-Type": "application/json"
}
  basicAuth = HTTPBasicAuth(
"ApiAdmin", "Admin123"
)

  response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False)
  print("Return Code:")
  print(response.status_code)
  print("Expected Outputs:")
  print(response.json())

```

Hier is het voorbeeld van de verwachte outputs.

Return Code:

200

Expected Outputs:

```
{'response': [{'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME0
```

## Systemcertificaat van een bepaald knooppunt verkrijgen via ID

Deze API geeft details van een systeemcertificaat van een bepaald knooppunt op basis van een gegeven hostnaam en ID.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/system-certificate/<ISE-Node-Hostname>/<ID-of-Certificate>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om het certificaat van een bepaald knooppunt op te halen op basis van de gegeven hostnaam en ID.

## Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v1/certs-docs?group=Certificates>

Servers

<https://10.106.33.92:44240> - Inferred Url

certs-api-controller the certs API

### Certificates

GET	/api/v1/certs/certificate-signing-request	Get all Certificate Signing Requests from PAN	▼	🔒
POST	/api/v1/certs/certificate-signing-request	Generate a Certificate Signing Request (CSR)	▼	🔒
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Get the certificate signing request for a given ID	▼	🔒
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Delete the certificate signing request for a given ID	▼	🔒
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id}	Export a CSR for a given CSR ID and hostname	▼	🔒
POST	/api/v1/certs/certificate-signing-request/intermediate-ca	Generate an intermediate CA CSR (certificate signing request)	▼	🔒
POST	/api/v1/certs/ise-root-ca/regenerate	Regenerate entire internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)	▼	🔒
POST	/api/v1/certs/renew-certificate	Renew certificates of OCSF responder and Cisco ISE Messaging Service	▼	🔒
POST	/api/v1/certs/signed-certificate/bind	Bind CA Signed Certificate	▼	🔒
GET	/api/v1/certs/system-certificate/{hostName}	Get all system certificates of a particular node	▼	🔒
GET	/api/v1/certs/system-certificate/{hostName}/{id}	Get system certificate of a particular node by ID	▲	🔒

This API provides details of a system certificate of a particular node based on given hostname and ID.

API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

```
from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "https://10.106.33.92/api/v1/certs/system-certificate/ISE-DLC-CFME02-PSN/5b5b28e4-2a51-495c-8413-610190e1" headers = {"Accept": "application/json", "Content-Type": "application/json"} basicAuth = HTTPBasicAuth("ApiAdmin", "Admin123") response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")
```



Opmerking: de ID is afkomstig van API-uitgangen in stap 3 van "Get All System Certificates Of A Particular Node", bijvoorbeeld, 5b5b28e4-2a51-495c-8413-610190e1070b is "Default self-signed saml server certificate - CN=SAML\_ISE-DLC-CFME02-PSN.cisco.com".

---

Hier is het voorbeeld van de verwachte outputs.

Return Code:

200

Expected Outputs:

```
{'response': {'id': '5b5b28e4-2a51-495c-8413-610190e1070b', 'friendlyName': 'Default self-signed saml server certificate - CN=SAML_ISE-DLC-CFME02-PSN.cisco.com'}}
```

Een lijst met alle vertrouwde certificaten opvragen

De API maakt een lijst van alle vertrouwde certificaten van ISE-cluster.

## Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/Trusted-certificate
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

## Stap 2: Zoek de URL die wordt gebruikt om vertrouwde certificaten op te halen.

The screenshot shows a list of API endpoints for the Cisco ISE system. The endpoint `GET /api/v1/certs/trusted-certificate` is highlighted with a red box. Below the list, there is a section for filtering and sorting attributes.

This API supports Filtering, Sorting and Pagination.

Filtering and Sorting are supported for the following attributes:

- friendlyName
- subject
- issuedTo
- issuedBy
- validFrom
  - Supported Date Format: yyyy-MM-dd HH:mm:ss
  - Supported Operators: EQ, NEQ, GT and LT
- expirationDate
  - Supported Date Format: yyyy-MM-dd HH:mm:ss
  - Supported Operators: EQ, NEQ, GT and LT
- status
  - Allowed values: enabled, disabled
  - Supported Operators: EQ, NEQ

Note: ISE internal CA certificates will not be exported.

## API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

```
<#root>
```

```
from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "https://10.106.33.92/api/v1/certs/trusted-certificate" headers = {"Accept": "application/json", "Content-Type": "application/json"} basicAuth = HTTPBasicAuth(
```



```
"ApiAdmin", "Admin123"
```

```
) response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")
```

Hier is het voorbeeld van de verwachte output.(weggelaten)

Return Code:

200

Expected Outputs:

```
{'response': [{'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certification Authority', 'subject': 'CN=VeriSign Class 3 Public Primary Certification Authority'}]}
```

## Vertrouwenscertificaat per ID verkrijgen

Deze API kan details van een vertrouwenscertificaat weergeven op basis van een gegeven ID.

Stap 1: Vereiste informatie voor een API-oproep.

Methode	KRIJGEN
URL	https://<ISE-PAN-IP>/api/v1/certs/Trusted-certificate/<ID-of-Certificate>
referenties	Open API-accountreferenties gebruiken
Koppen	Aanvaarden: aanvraag/json Content-Type: applicatie/json

Stap 2: Zoek de URL die wordt gebruikt om implementatieinformatie op te halen.

## Cisco ISE API - Certificates 1.0.0 OAS3

<https://10.106.33.92:44240/api/v1/certs-docs?group=Certificates>

Servers  
https://10.106.33.92:44240 - Inferred Url

certs-api-controller the certs API		⌵
<b>Certificates</b>		⌴
GET	/api/v1/certs/certificate-signing-request	Get all Certificate Signing Requests from PAN
POST	/api/v1/certs/certificate-signing-request	Generate a Certificate Signing Request (CSR)
GET	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Get the certificate signing request for a given ID
DELETE	/api/v1/certs/certificate-signing-request/{hostName}/{id}	Delete the certificate signing request for a given ID
GET	/api/v1/certs/certificate-signing-request/export/{hostname}/{id}	Export a CSR for a given CSR ID and hostname
POST	/api/v1/certs/certificate-signing-request/intermediate-ca	Generate an intermediate CA CSR (certificate signing request)
POST	/api/v1/certs/ise-root-ca/regenerate	Regenerate entire Internal CA certificate chain including root CA on the primary PAN and subordinate CAs on the PSNs (Applicable only for internal CA service)
POST	/api/v1/certs/renew-certificate	Renew certificates of OCSF responder and Cisco ISE Messaging Service
POST	/api/v1/certs/signed-certificate/bind	Bind CA Signed Certificate
GET	/api/v1/certs/system-certificate/{hostName}	Get all system certificates of a particular node
GET	/api/v1/certs/system-certificate/{hostName}/{id}	Get system certificate of a particular node by ID
This API provides details of a system certificate of a particular node based on given hostname and ID.		

API-URI

Stap 3: Hier is het voorbeeld van de Python-code. Kopieert en plakt de inhoud. Vervang de ISE IP, gebruikersnaam, wachtwoord. Opslaan als een python-bestand voor uitvoering.

Zorg voor een goede verbinding tussen ISE en het apparaat waarop het voorbeeld van de pythoncode wordt uitgevoerd.

<#root>

```
from requests.auth import HTTPBasicAuth import requests requests.packages.urllib3.disable_warnings() if __name__ == "__main__": url = "https://10.106.33.92/api/v1/certs/trusted-certificate/147d97cc-6ce9-43d7-9928-8cd0fa83e140" headers = {"Accept": "application/json", "Content-Type": "application/json"} basicAuth = HTTPBasicAuth("ApiAdmin", "Admin123") response = requests.get(url=url, auth=basicAuth, headers=headers, verify=False) print("Return Code:")
```



**Opmerking:** De ID is afkomstig van API-uitgangen in stap 3 van "Get List Of All Trusted Certificates", bijvoorbeeld, 147d97cc-6ce9-43d7-9928-8cd0fa83e140 is "VeriSign Class 3 Public Primary Certification Authority".

---

Hier is het voorbeeld van de verwachte outputs.

Return Code: 200 Expected Outputs: {'response': {'id': '147d97cc-6ce9-43d7-9928-8cd0fa83e140', 'friendlyName': 'VeriSign Class 3 Public Primary Certifi

Problemen oplossen

Om problemen op te lossen die betrekking hebben op de Open API's, stelt u **het niveau Log** voor deapiserice component in op **DEBUG** in **het** venster **Debug Log Configuration**.

Om debug in te schakelen, navigeer naar **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration > ISE Node > Appliance**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area is titled 'Debug Wizard' and 'Debug Log Configuration'. A table lists various components and their log levels. The 'api-service' component is selected, and its log level is set to 'DEBUG'. The 'Save' button is highlighted.

Component Name	Log Level	Description	Log file Name	Log Filter
accessfilter	INFO	RBAC resource access filter	ise-psc.log	Disabled
Active Directory	WARN	Active Directory client internal messages	ad_agent.log	Disabled
admin-ca	INFO	CA Service admin messages	ise-psc.log	Disabled
admin-infra	INFO	infrastructure action messages	ise-psc.log	Disabled
admin-license	INFO	License admin messages	ise-psc.log	Disabled
ai-analytics	INFO	AI Analytics	ai-analytics.log	Disabled
anc	INFO	Adaptive Network Control (ANC) debug...	ise-psc.log	Disabled
api-gateway	INFO	API Gateway native objects logs	api-gateway.log	Disabled
apiservice	DEBUG	ISE API Service logs	api-service.log	Disabled
bootstrap-wizard	INFO	Bootstrap wizard messages	psc.log	Disabled
ca-service	INFO	CA Service messages	caservice.log	Disabled

*Debug van API-service*

Als u debug-logbestanden wilt downloaden, navigeert u naar **Operations > Probleemoplossing > Downloadlogs > ISE PAN-knooppunt > Debug-logbestanden**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / Troubleshoot'. The left sidebar has 'Operations' highlighted. The main content area is titled 'Download Logs' and 'Debug Wizard'. A table lists various components and their log files. The 'api-service' component is selected, and its log files are listed. The 'api-service (all logs)' and 'api-service.log' files are highlighted.

Debug Log Type	Log File	Description	Size
Application Logs			
>	ad_agent (1) (100 KB)		
>	ai-analytics (11) (52 KB)		
>	api-gateway (16) (124 KB)		
>	api-service (13) (208 KB)		
<input type="checkbox"/>	api-service (all logs)	API Service debug messages	208 KB
<input type="checkbox"/>	api-service.log		12 KB
<input type="checkbox"/>	api-service.log.2024-03-24-1		4.0 KB
<input type="checkbox"/>	api-service.log.2024-04-07-1		4.0 KB

*Debug logs downloaden*

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.